

Exhibit 1

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

CARLO LICATA, individually and on behalf
of all others similarly situated,

Plaintiff,

v.

FACEBOOK, INC., a Delaware corporation,

Defendant.

Case No.

2015CH05427
CALENDAR/ROOM 07
TIME 00:00
Class Action

CLERK OF THE CIRCUIT COURT
DOMESTIC RELATIONS
DOROTHY BROWN
CLERK

RECEIVED

05 APR - 1 AM 11:52

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Carlo Licata brings this Class Action Complaint and Demand for Jury Trial (“Complaint”) against Defendant Facebook, Inc. to put a stop to its surreptitious collection, use, and storage of Plaintiff’s and the proposed Class’s sensitive biometric data. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

NATURE OF THE ACTION

1. Facebook operates the largest online social network in the world, with over one billion active users.
2. Users of Facebook’s platform can, among other things, upload and share photographs with friends and relatives. Once uploaded, users can organize and share their digital photographs by “tagging” (*i.e.*, identifying by name) Facebook friends who appear in the pictures.
3. In a purported attempt to make the process of tagging friends easier, Facebook launched a program in 2010 called “Tag Suggestions.” In its simplest form, Tag Suggestions functions by scanning photographs uploaded by the user and then identifying Facebook friends

who appear in the photos. If Tag Suggestions recognizes and identifies one of the user's Facebook friends, Facebook will suggest that individual's name and/or automatically tag them.

4. Unfortunately, Facebook actively conceals from its users that its Tag Suggestion feature actually uses proprietary facial recognition software to scan their uploaded photographs, locate their faces, extract unique biometric identifiers associated with their faces, and determine who they are. For instance, Facebook doesn't disclose its wholesale biometrics data collection practices in its privacy policies, nor does it even ask users to acknowledge them. Instead, Facebook merely hints at the underlying functionality behind Tag Suggestions—only describing the feature's use of facial recognition software on remote sections of its website. With millions of its users in the dark about the true nature of this technology, Facebook secretly amassed the world's largest privately held database of consumer biometrics data.

5. In addition to demonstrating a brazen disregard for its users' privacy rights, Facebook's actions also violate the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), which was specifically designed to protect Illinois consumers from practices like Facebook's. Specifically, Facebook's actions violated (and continue to violate) the BIPA because it did not:

- Properly inform Plaintiff or the Class in writing that their biometric data was being collected or stored, as required by the BIPA;
- Properly inform Plaintiff or the Class in writing of the specific purpose and length of time for which their biometric data was being collected, stored, and used, as required by the BIPA;
- Provide a publicly available retention schedule and guidelines for permanently destroying the biometric data of Plaintiff and the Class (who don't opt-out of "Tag Suggestions") as required by the BIPA; and most importantly,
- Receive a written release from Plaintiff or the members of the Class to collect, store, or use their biometric data as required by the BIPA.

6. Accordingly, this Complaint seeks an order (i) declaring that Facebook's conduct

violates the BIPA, (ii) requiring Facebook to cease the unlawful activities discussed herein, and (iii) awarding statutory damages to Plaintiff and the proposed Class.

PARTIES

7. Plaintiff Carlo Licata is a natural person and resident of Cook County and the State of Illinois.

8. Defendant Facebook, Inc. is a corporation existing under the laws of the State of Delaware, with its headquarters and principal place of business located at 1601 Willow Road, Menlo Park, California 94025. Facebook is also registered to conduct business in the State of Illinois (as entity number 66267067). Facebook conducts business throughout this County, the State of Illinois, and the United States.

JURISDICTION AND VENUE

9. This Court has personal jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 because Defendant conducts business transactions in Illinois, has committed tortious acts in Illinois, is registered to conduct business in Illinois, and has offices located in Illinois. Additionally, this Court has personal jurisdiction over Plaintiff Licata because he is a resident of the State of Illinois.

10. Venue is proper in Cook County because Defendant is registered to conduct business in Illinois, conducts business transactions in Cook County, entered into a contract with Plaintiff Licata in Cook County, and the causes of action arose, in substantial part, in Cook County. Venue is additionally proper because Plaintiff Licata resides in Cook County and Facebook has offices located in Cook County.

FACTUAL BACKGROUND

I. The Use of Biometrics and Consumer Privacy.

11. “Biometrics” refers to technologies used to identify an individual based on unique physical characteristics. One of the most prevalent uses of biometrics is facial recognition technology, which works by scanning an image for human faces (or scanning an actual person’s face), extracting facial feature data, and comparing them against information stored in a “faceprint database.” If a database match is found between the extracted facial data and the “biometric identifiers” (*i.e.*, details about the face’s geometry), a person may be identified.

12. The recent development of sophisticated facial recognition software has generated unique opportunities for commercial application of the technology, while also raising serious concerns about its threat to consumer privacy. During a 2012 hearing of the United States Senate Subcommittee on Privacy, Technology, and the Law, one expert testified that facial recognition technology takes the “risks inherent in . . . biometrics to a new level because Americans cannot take precautions to prevent the collection of their image,” and that “[f]ace recognition allows for covert, remote and mass capture and identification.”¹

13. In discussing the dangers associated with obtaining and storing a person’s facial biometric identifiers, the expert further noted that someone with access to an individual’s faceprint can use it to find their “name, . . . social networking account and . . . can [be used to] find and track [them] in the street, in the stores [they] visit, the government buildings [they]

¹ *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012) (statement of Jennifer Lynch, Staff Attorney, Electronic Frontier Foundation), available at https://www.eff.org/files/filenode/jenniferlynch_eff-senate-testimony-face_recognition.pdf.

enter, and the photos [their] friends post online.”²

14. During the hearing, captioned “What Facial Recognition Technology Means for Privacy and Civil Liberties,” Senator Al Franken asserted that “there is nothing inherently right or wrong with [facial recognition technology, but] if we do not stop and carefully consider the way we use [it], it may also be abused in ways that could threaten basic aspects of our privacy and civil liberties.”³ For example, Sen. Franken continued, it is possible to use the technology to identify people at a distance and in crowds and could be “abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution.”⁴

15. Federal regulators have voiced similar concerns. In late 2011, the Federal Trade Commission (“FTC”) hosted a series of wide-ranging discussions with researchers, academics, and industry representatives (including Facebook) about facial recognition technologies. Among the topics examined were the potential hazards of a third party maliciously breaching a database of biometric information. The consequences of such a breach would be especially harmful because unlike numerical identifiers (*e.g.*, Social Security numbers), which can be replaced or re-assigned, biometrics are biologically unique to each person and therefore, once exposed, a victim has no recourse to prevent becoming victim to misconduct like identity theft and unauthorized tracking.

16. From these discussions, the FTC formulated a “Best Practices” guide for

² *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012) (statement of Sen. Al Franken, Chairman, Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary), *available at* http://www.franken.senate.gov/?p=press_release&id=2144.

³ *Id.*

⁴ *Id.*

companies using facial recognition technology.⁵ One consistent theme throughout the FTC's guide is the necessity that companies provide consumers with the option to affirmatively consent to the collection of their biometric identifiers *before* ever scanning and extracting biometric data from digital photographs.

17. Concentrating on social networks in particular, the FTC noted that “[b]ecause this [facial recognition technology] use is not currently within the context of consumers’ relationship with the social network, when the company first rolls out this feature and begins analyzing users’ photos to gather biometric data, it should provide users with a clear notice, outside of a privacy policy, about how the feature works, what data it collects, and how that data will be used. Companies should also provide consumers with an easy to find, meaningful choice not to have their biometric data collected and used for facial recognition.”⁶

18. As explained below, obtaining the consent of users and following the FTC’s guidelines is precisely what Facebook *did not do* when it rolled out its facial recognition program. Not only do Facebook’s actions controvert industry best practices, they also violate the privacy rights of Illinois residents.

II. Illinois’s Biometric Information Privacy Act.

19. In 2008, Illinois enacted the BIPA in recognition of the “very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information.” Illinois House Transcript, 2008 Reg. Sess. No. 276. As such, the BIPA makes it unlawful for a company to, among other things, “collect, capture, purchase, receive through trade, or otherwise obtain a

⁵ See *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), available at <http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf>.

⁶ *Id.*

person's or a customer's biometric identifiers⁷ or biometric information, unless it first:

- (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
- (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
- (3) receives a written release executed by the subject of the biometric identifier or biometric information."

740 ILCS 14/15(b).

20. The BIPA also establishes standards for how companies must handle Illinois consumers' biometric identifiers and biometric information. *See, e.g.*, 740 ILCS 14/15(c) – (d). For instance, the BIPA prohibits selling, leasing, trading, or otherwise profiting from a person's biometric identifiers or biometric information, 740 ILCS 14/15(c), and requires that companies develop a written policy—made available to the public—establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting such identifiers or information has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS 14/15(a).

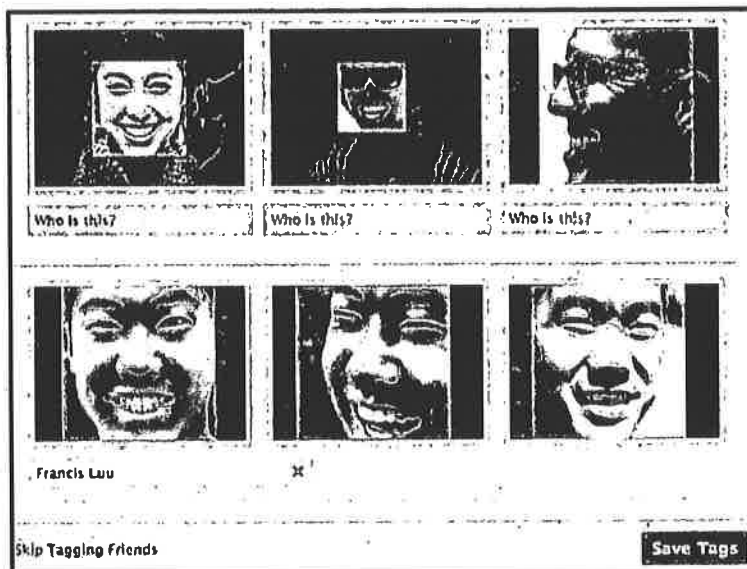
III. Facebook Violates the Biometric Information Privacy Act.

21. In 2010, Facebook launched a program dubbed "Tag Suggestions" that claimed to "automate the process of identifying and, if the user chooses, tagging friends in the photos he or she uploads."⁸

⁷ The BIPA's definition of "biometric identifier" expressly includes information collected about the geometry of the face (*i.e.*, facial data obtained through facial recognition technology). *See* 740 ILCS 14/10.

⁸ *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012) (statement of Robert Sherman, Manager of Privacy and Public Policy, Facebook,

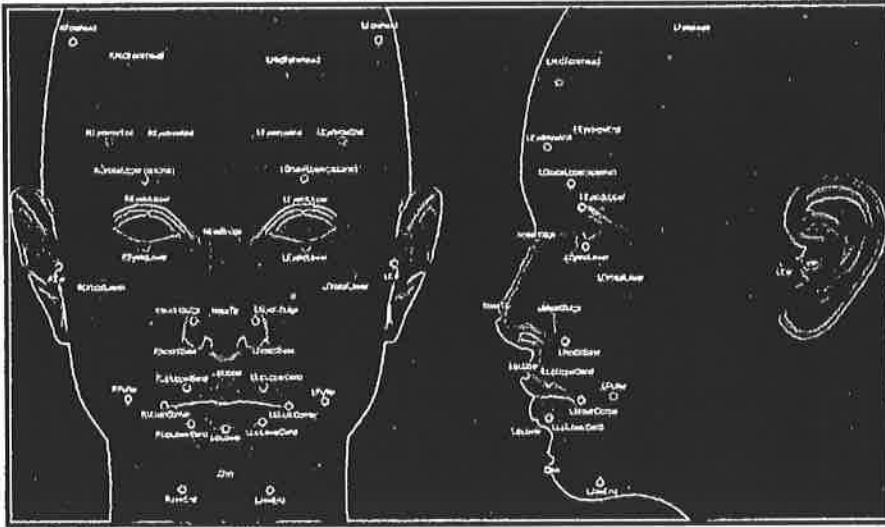
22. Unbeknownst to the average consumer, Tag Suggestions relies on proprietary facial recognition technology to scan photographs, locate a person's face, and determine who he or she is. Figure 1 below depicts an example of how Tag Suggestions would appear to a user on Facebook's website.



(Fig. 1.)

23. The technology works by calculating similarities in previously uploaded photographs of a person and creating a unique standalone faceprint of the individual, which Facebook refers to as a “template.”

24. “Template” data stored by Facebook is derived in part from biometric identifiers collected from the image of a person's face. According to Facebook's website, these biometric identifiers include information about the geometry of a person's face, including the distance between the eyes, nose, and ears. (See Figure 2 on the following page, showing an example of the geometric data points of a human face.)



(Fig. 2.)

25. Without even informing its users—*let alone obtaining their informed written consent*—when Facebook activated Tag Suggestions, it automatically enrolled its users into its facial recognition program and began creating templates from their uploaded photographs and previously tagged pictures. Because they were only allowed to opt out of the program *after the fact*, Facebook users unwittingly had their photographs scanned and processed to collect their biometric identifiers—a practice that continues to this day.

26. Criticism of Facebook's program followed shortly after its initial implementation. Data protection officials in Europe alleged that Facebook was illegally compiling a database of biometric data without user consent. After an investigation by the European Union, Facebook agreed to discontinue its facial recognition program in Europe in 2012.

27. In the United States, Congressional inquiries were held. Speaking about Facebook's Tag Suggestions program, Sen. Franken asserted that, "Facebook may have created the world's largest privately-held database of faceprints—without the explicit consent of its users."⁹ And in fact, Sen. Franken was right.

⁹

See What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing

- A. *Facebook never requires users to acknowledge its biometric data collection practices, never obtains their express written consent to collect the same, and, instead, hides the fact that it systematically collects users' biometrics.*

28. Since Tag Suggestions debuted in 2010, Facebook has been calculatedly elusive in explaining how the technology works or how it would be used to collect millions of users' biometric data (*i.e.*, their faceprints).

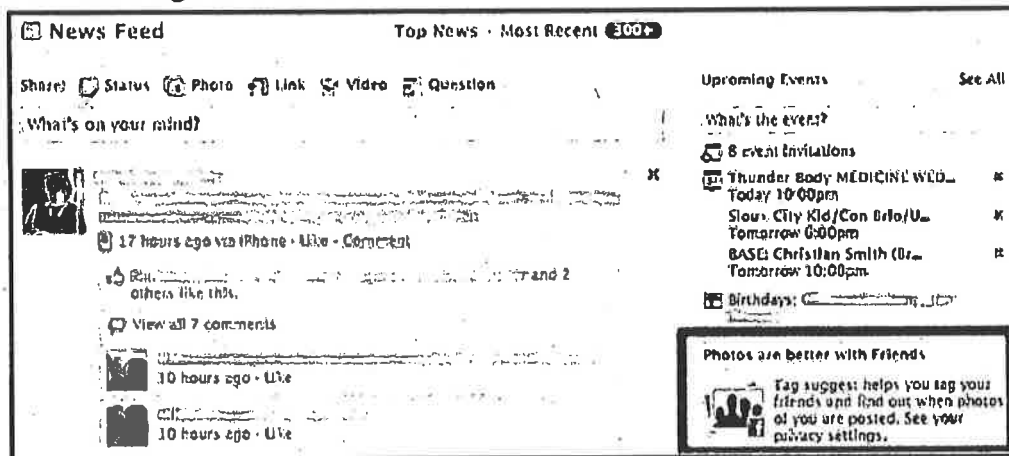
29. In fact, since the Tag Suggestions feature was rolled out, Facebook has kept its biometrics data collection practices out of its privacy policies and has instead placed ambiguous statements about the true nature of its Tag Suggestions program on remote sections of its website (such as in its "Help Center" or the now defunct "Notes" sections). Uncovering these remote sections requires a user to not only know about Tag Suggestions in the first place, but also affirmatively seek out more information through multiple layers of additional pages.

30. Worse still, Facebook doesn't even require users to acknowledge its collection of their biometric data, let alone receive a written release from users before collecting their faceprints.

31. Instead, Facebook markets its Tag Suggestions technology as a convenience feature that allows users to automate the process of identifying and tagging friends in the photos they upload. For instance, in or around June 2011 (*after* Facebook had already collected millions of users' faceprints without explicit permission), advertisements for Tag Suggestions started to appear alongside commercial ads, alerts, event listings, and other updates with the innocuous heading "Photos are better with Friends"—which served to decrease the likelihood that consumers would notice or believe the item to be an important or relevant point of information.

Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary, 112th Cong. 1 (2012) (statement of Sen. Al Franken, Chairman, Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary), *supra* note 2.

(See Figure 3 below showing a screenshot of a “Photos are better with Friends” advertisement.)



(Fig. 3.)

The text, highlighted in red in Figure 3, falls considerably short of the FTC’s guidance that companies should “provide users with a clear notice, outside of a privacy policy, about how the [facial recognition] feature works, what data it collects, and how that data will be used.”¹⁰

32. Even more problematic, Facebook’s website does not have a written, publicly-available policy identifying its retention schedule, nor guidelines for permanently destroying users’ (who don’t opt-out of “Tag Suggestions”) biometric identifiers when the initial purpose for collecting or obtaining such identifiers (or information has been satisfied or within three years of the individual’s last interaction with Facebook) as required by the BIPA.

33. By and through the actions detailed above, Facebook not only disregarded its users’ privacy rights, but it also violated their statutorily protected rights to control the collection, use, and storage of their sensitive biometric data.

IV. Plaintiff Licata’s Experience.

34. Licata has been a member of Facebook’s social network since 2009. Since then, Licata has uploaded photographs to his account—including those used for his profile pictures—

¹⁰ See note 5, *supra*.

and has frequently been tagged in photos by friends.

35. Licata never consented, agreed, or gave permission—written or otherwise—to Facebook to collect or store biometrics identifiers associated with his faceprint. Further, Licata was never provided with nor ever signed a written release allowing Facebook to collect or store his biometric identifiers derived from his faceprint.

36. Worse still, Facebook never even informed Licata by written notice or otherwise that he could prevent Facebook from collecting or storing biometric identifiers derived from his faceprint.

37. Likewise, Licata was never provided with an opportunity to prohibit or prevent Facebook from collecting or storing biometric identifiers derived from his faceprint.

38. Nevertheless, when Licata uploaded photographs to his account and made them his profile pictures and also when he was tagged in photos, Facebook scanned those photos, located his face, determined who he was, and created a unique faceprint or “template” for him based on his biometric identifiers, including his facial geometry. Facebook subsequently stored Licata’s faceprint in its databases.

CLASS ALLEGATIONS

39. **Class Definition:** Plaintiff Licata brings this action pursuant to 735 ILCS 5/2-801 on behalf of himself and a class of similarly situated individuals, defined as follows:

All residents of the State of Illinois who had their faceprints collected, captured, received, or otherwise obtained by Facebook while residing in Illinois.

The following people are excluded from the Class: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant’s subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and its current or former employees, officers and directors; (3) persons who properly

execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

40. **Numerosity:** The exact number of Class members is unknown to Plaintiff at this time, but it is clear that individual joinder is impracticable. Defendant has collected, captured, received, or otherwise obtained biometric identifiers or biometric information from thousands of consumers who fall into the definition of the Class. Ultimately, the Class members will be easily identified through Defendant's records.

41. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

- a) whether Facebook collected or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;
- b) whether Facebook properly informed Plaintiff and the Class that it collected, used, and stored their biometric identifiers or biometric information;
- c) whether Facebook obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store Plaintiff's and the Class's biometrics identifiers or biometric information;
- d) whether Facebook has sold, leased, traded, or otherwise profited from Plaintiff's and the Class's biometrics identifiers or biometric information;
- e) whether Facebook developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometrics information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of their last interaction, whichever occurs first;

- f) whether Facebook used Plaintiff's and the Class's biometric identifiers or biometric information to identify them; and
- g) whether Facebook's violations of the BIPA were committed intentionally, recklessly, or negligently.

42. **Adequate Representation:** Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to those of the other members of the Class.

43. **Appropriateness:** This class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class are likely to have been small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

FIRST CAUSE OF ACTION
Violation of 740 ILCS 14/1, *et seq.*
(On Behalf of Plaintiff and the Class)

44. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

45. The BIPA makes it unlawful for any private entity to, among other things, “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifiers or biometric information, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; *and* (3) receives a written release executed by the subject of the biometric identifier or biometric information” 740 ILCS 14/15(b) (emphasis added).

46. Facebook is a Delaware corporation and thus qualifies as a “private entity” under the BIPA. *See* 740 ILCS 14/10.

47. Plaintiff and the Class are individuals who had their “biometric identifiers” collected by Facebook’s facial recognition software (in the form of their facial geometries extracted from uploaded digital photographs), as explained in detail in Section III. *See* 740 ILCS 14/10.

48. Plaintiff’s and the Class’s biometric identifiers were used to identify them, and therefore constitute “biometric information” as defined by the BIPA. *See* 740 ILCS 14/10.

49. Facebook systematically and automatically collected, used, and stored their biometric identifiers or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

50. In fact, as explained in Section III.A, Facebook didn’t properly inform Plaintiff or the Class in writing that their biometric identifiers or biometric information were being collected

and stored, nor did it inform them in writing of the specific purpose and length of term for which their biometric identifiers or biometric information was being collected, stored, and used as required by 740 ILCS 14/15(b)(1) – (2).

51. In addition, Facebook does not publicly provide a retention schedule or guidelines for permanently destroying its users' (who don't opt-out of "Tag Suggestions") biometric identifiers and biometric information as specified by the BIPA. *See* 740 ILCS 14/15(a).

52. By collecting, storing, and using Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Facebook violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in the BIPA, 740 ILCS 14/1, *et seq.*

53. On behalf of himself and the Class, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Facebook to comply with the BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (2) statutory damages of \$5,000 for the intentional and reckless violation of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of \$1,000 pursuant to 740 ILCS 14/20(1) if the Court finds that Facebook's violations were negligent; and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Carlo Licata, on behalf of himself and the Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Licata as representative of the Class, and appointing his counsel as Class

Counsel;

B. Declaring that Facebook's actions, as set out above, violates the BIPA, 740 ILCS 14/1, *et seq.*;

C. Awarding statutory damages of \$5,000 for the intentional and reckless violation of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of \$1,000 pursuant to 740 ILCS 14/20(1) if the Court finds that Facebook's violations were negligent;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, *inter alia*, an order requiring Facebook to collect, store, and use biometric identifiers or biometric information in compliance with the BIPA;

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

G. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Respectfully submitted,

CARLO LICATA, individually and on behalf of
all others similarly situated,

By: 

One of Plaintiff's Attorneys

Dated: April 1, 2015

Jay Edelson
jedelson@edelson.com
Rafey S. Balabanian
rbalabanian@edelson.com
Benjamin H. Richman
brichman@edelson.com

J. Dominick Larry
nlarry@edelson.com
David I. Mindell
dmindell@edelson.com
EDELSON PC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378
Firm ID: 44146